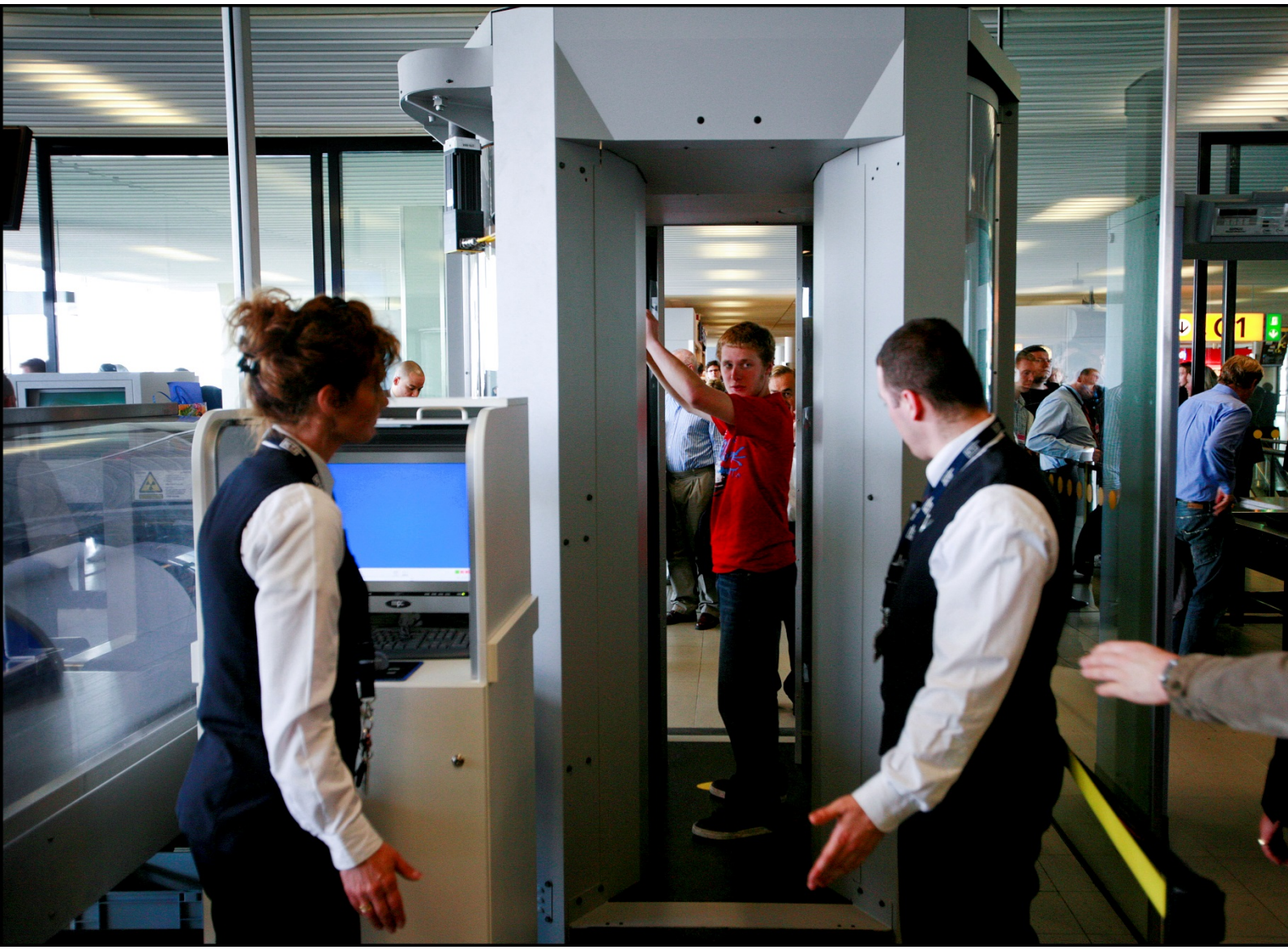
Rathenau Instituut

What do citizens think about the use of sensor data for safety and quality of life?

A conceptual framework for engagement with the public



Article

Authors
Marijn Biesiot, Erik de Bakker, Tim Jacquemard & Rinie van Est

Editor
Frank Steverink

Illustrations and photographs
Rikkers Infographics

Cover photograph
The Netherlands, Schiphol Airport, 15 May 2007, Introduction / world premiere of the Security Scan. A full-body scanner that detects objects carried on a person's body by emitting harmless electromagnetic radiation. The scanner has made the traditional manual pat-down unnecessary. Photograph Michael Kooren / Hollandse Hoogte

Preferred citation form:
Biesiot, M., E. de Bakker, T. Jacquemard & R. van Est (2019).
What do citizens think about the use of sensor data for safety and quality of life? A conceptual framework for engagement with the public. The Hague: Rathenau Instituut

The Rathenau Instituut has been commissioned by the Dutch National Police Corps to investigate how citizens view the use of sensor data to improve safety and quality of life. To do so, we organised six focus groups of Dutch citizens and encouraged discussion among them by presenting a number of scenarios. The focus groups were set up to help us understand the opinions and arguments of various members of society.

The aim is for the focus groups to discuss as many aspects of public perception as possible. To achieve this, we draw on the outcomes of earlier studies. This article reviews what other researchers have concluded about citizens' perspectives on sensors and sensor data. We introduce a conceptual framework to help us prepare for and set up the focus groups in accordance with the above-standing aim.

For more information about this study, see our website:
https://www.rathenau.nl/nl/digitale-samenleving/nieuw-onderzoek-sensordata-voor-veiligheid-en-leefbaarheid (in Dutch)

A previous article about this study was entitled: Eyes and ears everywhere – *Using sensor data for safety and quality of life*
https://www.rathenau.nl/en/digital-society/using-sensor-data-safety-and-quality-life

Introduction

When full-body security scanners were introduced at Schiphol Airport ten years ago, a fuss ensued about "scanners that show you naked". Journalists and opinion-makers raised questions. Was it not going too far to ask passengers to "expose" themselves in the scanner? Could they trust security staff to handle the image data with due care? Could they be absolutely certain that the scanners were not harmful to health? Were scanners even the right means in the fight against terrorism?

These questions highlight factors – for example health safety and personal data protection – that may influence whether or not the public regards the use of sensors as acceptable. In this article, we search for other factors of this kind. Examining what we already know about public perceptions will help us to prepare our focus groups, where small groups of ordinary Dutch people will discuss various situations in which sensors[1] and sensor data are used to improve safety and quality of life.[2]

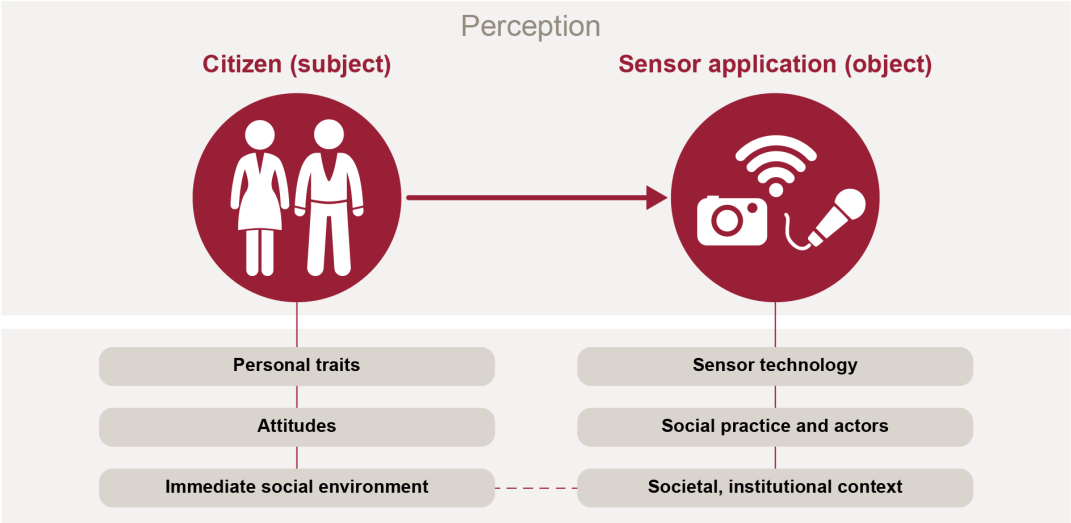
1 By "sensors", we mean digital measuring instruments that collect data about the physical and social environment. Examples include digital cameras and GPS on a smartphone.

2 The study "Public perspective on use of sensor data for safety and quality of life" [*Burgerperspectief op inzet sensordata voor leefbaarheid en veiligheid*] focuses on safety and quality of life in a broad sense. "Quality of life" refers to minor infractions, such as littering. On the other end of the spectrum are more serious misdemeanours that create a major sense of *insecurity*, such as mugging, threats, assault, and serious forms

What do they think of these situations? What aspects do they consider, and what are the reasons for their opinions?

In this article, we introduce a conceptual framework for public attitudes towards the use of sensors and sensor data. Our starting point is: *someone* (a subject) has an opinion about *something* (an object). In other words, *a private individual* finds a *sensor application* acceptable or unacceptable. The subject and the object of this perception is the first level of our conceptual framework.

Figure 1 Introduction to conceptual framework



Source: Rathenau Instituut

Whether or not people find a sensor application acceptable may depend on their individual characteristics (e.g. is someone open to sharing information?) and on the features of the sensor application (e.g. what sort of information is it collecting?). The conceptual framework helps us to seek out relevant factors in real-life examples and in the scholarly literature and then arrange these factors logically in dimensions that pertain to the subject or object.

We first explain why this article focuses on “top-down” surveillance and not on the other types of sensor surveillance noted in the previous article, “Eyes and ears everywhere”. We then study two real-life examples of sensor surveillance and identify three important dimensions of sensor applications. Next, we search the academic literature for factors that can influence the extent to which people find a sensor application acceptable (or unacceptable). We use our findings to fine-tune our conceptual framework. Finally, we revisit the various types of sensor

of crime such as drug trafficking and trafficking in human beings. This study therefore concentrates on the task of the police, which primarily involves enforcing the rule of law and providing assistance in the event of an emergency. When deciding whether to discuss a real-life example, we therefore always ask ourselves whether it involves a situation in which one would call the police.

surveillance and formulate a number of suggestions for the focus group conversations based on the findings of this article.

Sensor surveillance

The full-body security scanners at Schiphol Airport are an example of how surveillance sensors are employed to improve security. Surveillance involves the "purposeful, systematic and routine" search for personal details.[3] In this particular case the scanners at the airport search for objects on a person's body, but sensors can collect all kinds of data (such as locations, fingerprints, sounds and images).

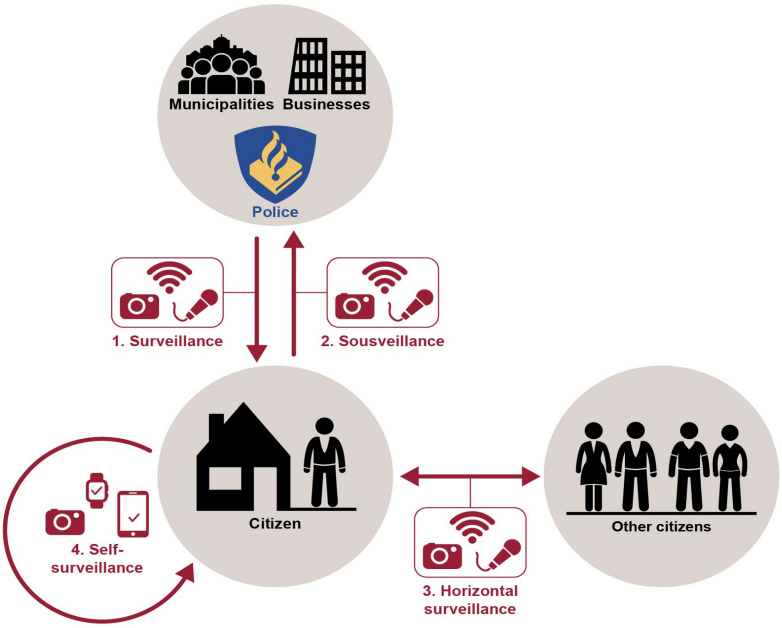
In the previous article, we saw that "sensor surveillance" is a dynamic and interactive process. It is not controlled from a single, central point.[4] Individuals, government organisations and companies monitor one another and are themselves monitored. In addition to the authorities and companies monitoring individuals (*top-down surveillance*), individuals keep an eye on organisations (*sousveillance*) and other people (*horizontal surveillance*). Finally, individuals use sensor-based devices and applications to help them stick to the rules for safety/security and quality of life (*self-surveillance*). Figure 2 illustrates these four types of sensor surveillance.

In this article, we focus on top-down surveillance. That is because we know more about what people think of "top-down" sensor surveillance than about the other types of sensor surveillance. The factors we encounter in this context may also play a role in other types of sensor surveillance. We will return to this point at the end of this article.

3 Boutellier, H (2015). *Het seculiere experiment. Hoe we van God los gingen samenleven.* Amsterdam: Uitgeverij Boom, chapter 4

4 Idem

Figure 2 Four types of surveillance using sensors



Source: Rathenau Instituut

Questions about surveillance in practice

We examine two real-life examples in which sensors and sensor data are used to improve security and quality of life: the full-body security scanners at Schiphol Airport, and a trial involving sensor data in the town of Roermond. We also consider some of the issues that opinion-makers raise.

Full-body security scanners at Schiphol Airport

The full-body security scanners at Schiphol Airport check that passengers are not carrying prohibited items on their bodies. In 2009, a Nigerian carrying a bomb attempted to blow up a plane flying from Schiphol to Detroit. His attempt failed. Since then, airports have attempted to prevent further attacks by employing a growing number of security scanners.[5] The sensors used at Schiphol Airport emit millimetre waves that pass through clothing but are reflected by the skin and other materials,[6] making it possible to detect suspicious objects.

Schiphol first used a full-body security scanner to check a limited number of passengers in 2007.[7] The scanners revealed prohibited materials hidden under

5 'Hirsch Ballin wil bodyscan invoeren'. *Het Parool* website, 29 December 2009. https://www.parool.nl/binnenland/hirsch-ballin-wil-bodyscan-invoeren~a273592/
6 'Prepare for security'. Schiphol website, consulted on 22 October 2018. https://www.schiphol.nl/nl/security-check/
7 *Kamerstukken II 2006/2007*, 24 804, no. 44

clothing, but also a three-dimensional black and white image of the passenger's naked body, quickly earning them the nickname "naked scanners".[8] To ensure privacy, a security officer assessed the image in a separate room. The passenger's face was blurred and the image was deleted after assessment. Schiphol modified its use of full-body scanners after objections were raised against the "naked images" of passengers.

The security scanners at Schiphol now indicate any suspicious object on an image of a generic human figure with no features. This image is visible on the spot to both the passenger and the security officer.[9] The results of the scanning procedure are therefore transparent to passengers. Schiphol says the following on its website: "The scan is analysed by a computer and not a human. It cannot look through your body or take nude photos of you, which ensures that your privacy is guaranteed."[10]

Civil society organisations and opinion-makers have raised various critical questions about the full-body scanners at Schiphol Airport. In 2009, Dutch civil rights organisation Bits of Freedom claimed that the "naked scanners" violated passengers' privacy and physical integrity[11] by subjecting them to a "digital strip-search". How can we know for sure that the airport security officers deal respectfully with the images?[12] Bits of Freedom also pointed out that the scanners are not flawless, expensive to operate, and only eliminate some of the risk of attack.[13] In the summer of 2015, Ancilla van de Leest, then the leader of the Pirate Party (a Dutch political party that campaigns for digital civil rights), addressed the rules and procedures that apply to pregnant women undergoing the scans.[14]

In the opinion of Bits of Freedom and Van de Leest full-body scanners have less desirable aspects. They question whether the use of these scanners is an effective instrument in the fight against terrorism. Can measures such as the security scan actually prevent attacks? On the other hand, what would the public think if a full-body scanner could have prevented an attack but was not used?

---

8 See for example 'Naaktscan of bodyscan?'. *De Volkskrant* website, 18 November 2010. https://www.volkskrant.nl/nieuws-achtergrond/naaktscan-of-bodyscan-~q1dd14d9/

9 'Wat ik zie als jij in de securityscan staat'. Schiphol website, 14 July 2017. https://nieuws.schiphol.nl/wat-ik-zie-als-jij-in-de-securityscan-staat/

10 'Security check' (under Frequently Asked Questions). Schiphol website, consulted on 22 October 2018. https://www.schiphol.nl/nl/security-check/

11 Van Daalen, O. Persbericht: 'Bits of Freedom: Naaktscanners niet introduceren'. Bits of Freedom website, 30 December 2009. https://www.bitsoffreedom.nl/2009/12/30/persbericht-bits-of-freedom-naaktscanners-niet-introduceren/

12 'Open brief aan de Minister van Justitie'. Bits of Freedom website, 30 December 2009. https://www.bitsoffreedom.nl/2009/12/30/persbericht-bits-of-freedom-naaktscanners-niet-introduceren/

13 'Open brief aan de Minister van Justitie'. Bits of Freedom website, 30 December 2009. https://www.bitsoffreedom.nl/2009/12/30/persbericht-bits-of-freedom-naaktscanners-niet-introduceren/

14 Van de Leest, A. 'Schiphol dwingt je onterecht in de naaktscanner'. Joop website, 1 June 2015. https://joop.bnnvara.nl/opinies/schiphol-dwingt-je-onterecht-in-de-naaktscanner

Sensors that register points in Roermond

The town of Roermond is troubled by shoplifters and pickpockets, many of whom come from Eastern Europe. In 2017, police recorded 456 cases of pickpocketing and 383 cases of shoplifting.[15] Roermond is an attractive location for this type of crime because it is home to Europe's largest designer outlet centre, which attracts large numbers of Asians and Russians (who often carry cash). About 8 million people flock to Designer Outlet Roermond every year.[16] Combined with its other attractions, Roermond – a town of less than sixty thousand inhabitants – attracts a total of about fourteen million visitors annually.

Despite the use of private security guards, cooperation with the German and Romanian police and amendments to local ordinances, there has been no significant improvement in the number of incidents over the past three years.[17] The police are now running a "living lab" in which they are testing whether a new approach using sensor technology can bring about a change in this situation.[18] In July 2018, the police force, the City of Roermond, Eindhoven University of Technology and the Office of the Public Prosecutor began a trial in which sensor data are correlated to track travelling groups of criminals as soon as possible.

The living lab in Roermond involves intelligent sensor applications that recognise patterns as well as an associated points system.[19] Analysis of correlated data may produce a "suspect profile". Although at this point the trial does not include all possible sensors and sensor data, the idea is as follows: ANPR cameras positioned above the access roads to Designer Outlet Roermond record the number plates and number of passengers of every car. If a car has a Romanian number plate, it is assigned ten points. If the car is a white rental and has four passengers, additional points are assigned. Wi-Fi trackers then analyse mobile phone data and track other movement patterns.[20] If enough points have been assigned to persons (or a group of persons), the police take action. Steps may include heightened scrutiny if the vehicle is detected again in the coming week, using information boards to alert visitors to the presence of pickpockets, asking security to step up surveillance or, if the same vehicle was involved in previous incidents, follow-up by the police themselves, for example by engaging with the driver. The idea is that joint action based on sensor data could also act as a deterrent.

15 Driessen, G. 'Jacht op de zakkenroller'. In: *de Limburger* 12 July 2018.
16 'Bijna 4000 Chinezen komen shoppen in Designer Outlet Roermond'. Roermond Nieuws website, 1 May 2018. https://roermond.nieuws.nl/nieuws/81749/bijna-4000-chinezen-komen-shoppen-designer-outlet-roermond/
17 Driessen, G. 'Jacht op de zakkenroller'. In: *de Limburger* 12 July 2018.
18 'Zakkenrollers herkennen dankzij data-koppeling'. Dutch Police Corps website, 11 July 2018. https://www.politie.nl/nieuws/2018/juli/11/00-zakkenrollers-herkennen-dankzij-data-koppeling.html
19 Andringa, R. 'Politie wil zakkenrollers en plofkrakers vangen met data'. NOS website, 17 September 2018. https://nos.nl/artikel/2250767-politie-wil-zakkenrollers-en-plofkrakers-vangen-met-data.html
20 Van Teeffelen, K. 'Met camera's en sensors is een winkeldief straks op grote afstand te herkennen'. *Trouw* website 17 September 2018. https://www.trouw.nl/samenleving/met-camera-s-en-sensors-is-een-winkeldief-straks-op-grote-afstand-te-herkennen~acdee79e/

At the present time, early 2019, the aforementioned correlation of sensor data and joint action in response to suspect profiles have not been implemented in full. Number plates are being recorded, but not the number of passengers per car. Also, there is no tracking of movement patterns as of yet.

Local politicians support this living lab. Civil society organisations however, have been more critical. In September 2018, digital civil rights organisation Bits of Freedom worried that people would be marked as suspicious merely for behaving differently or for fitting certain criteria. If such systems become commonplace in the future, according to Bits of Freedom, there is potentially nothing that will escape the watchful eye of the authorities. Every form of misconduct could then be punished by automated means, without the intervention of humans.[21] But what if innocent people are mistakenly identified as suspects (false positives)? Who is responsible for any adverse consequences? An algorithm? The living lab in Roermond does not involve automated sanctions, but Bits of Freedom sees the risk of a slippery slope.

Lokke Moerel, professor of Global IT Law at Tilburg University, wonders whether there are less invasive ways to track pickpockets than by collecting data about every passer-by.[22] Her question is whether gathering data on large numbers of people is in due proportion to the arrest of a small number of pickpockets.

In November 2018, the Dutch Data Protection Authority (DPA) pointed out that digital tracking of individuals on the street, in shopping centres and public or semi-public places is only permitted under strict conditions. Wi-Fi tracking is considered personal data and is therefore subject to privacy rules. “There are practically no legitimate reasons to track shoppers or travellers,’’ according to chairman of the Dutch DPA, Aleid Wolfsen. “There are also less intrusive ways to achieve the same aim without invading privacy.” [23]

Three dimensions of sensor applications

The two real-life examples above reveal various societal issues associated with surveillance. These issues involve three important dimensions of sensor applications:

1. the functioning of the sensor technology itself;

21 Zenger, R. ‘Experimenteren zonder visie is onverantwoord en gokken met onze toekomst’. Bits of Freedom website, 18 September 2018. https://www.bitsoffreedom.nl/2018/09/18/experimenteren-zonder-visie-onverantwoord-en-gokken-met-onze-toekomst/

22 Hendriks, J. ‘Boeven vangen met big data, mag dat?’. Univers website, 26 September 2018. https://universonline.nl/2018/09/26/boeven-vangen-met-big-data-mag-dat

23 ‘Bedrijven mogen mensen alleen bij hoge uitzondering met wifitracking volgen’. Dutch Data Protection Authority website, 30 November 2018. https://autoriteitpersoonsgegevens.nl/nl/nieuws/bedrijven-mogen-mensen-alleen-bij-hoge-uitzondering-met-wifitracking-volgen

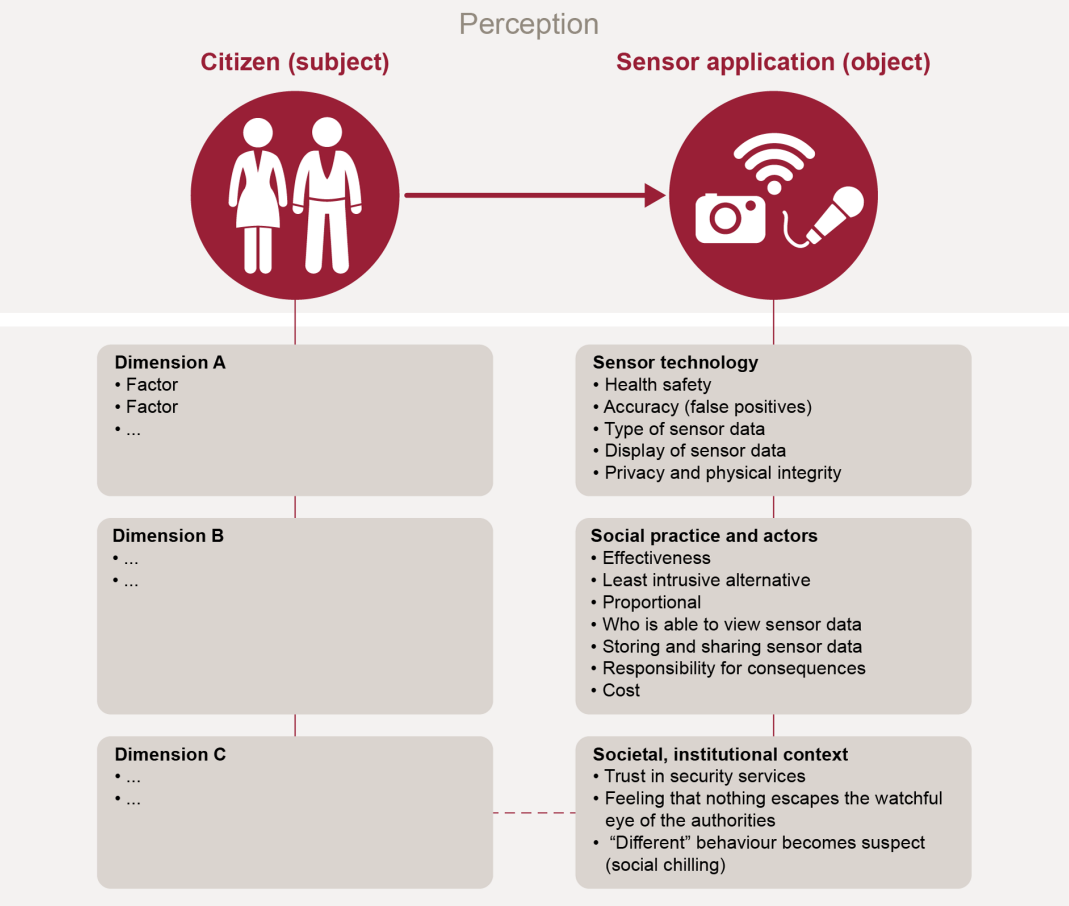
2. the social practice in which the technology is applied and the actors involved;
3. the broader societal, cultural and institutional context in which the practice has arisen.

Public perceptions may involve any and all of these dimensions, and, consequently, any and all of the factors that influence such perceptions. Figure 3 shows our conceptual framework with the relevant factors drawn from our real-life examples. Concerns about the health risks of full-body scanners, for example, are related to the functioning of the technology itself. The passengers' wish to see, on the spot, how the scanner displays data about their bodies, impacts the way in which Schiphol Airport actually applies the technology. Trustworthiness of security services refers to the societal and institutional context in which the technology is applied. In real-life situations, the three dimensions are interrelated. The extent to which a sensor application infringes people's private lives may, for example, be related to the design of the technology itself, but also to the procedures followed in the specific practice in which the technology is used.

In the second dimension (social practice), the term 'actors' refers to all the parties involved in the sensor technology. They include the person or organisation that collects sensor data, the analyst who works with the output of the software that correlates and analyses all the sensor data, and the police officer on the beat or the security guard in the shop who takes action. In addition, sensor data can be collected about different people or groups of people, for example everyone walking down the high street or driving past an ANPR camera.

In our real-life examples, software automatically collects and analyses sensor data, but there is always a police officer or security guard who studies the information and decides what action is needed. In other words, people continue to play a decisive role within the system of collecting, analysing and applying sensor data.

Figure 3 Factors that feature in the real-life examples



Source: Rathenau Instituut

Later in this article, we add factors related to the subject to our conceptual framework. First, however, we take a look at Dutch research.

Factors identified in Dutch research

Every year, Capgemini investigates Dutch attitudes towards trends in the security domain. Figures from its publication *Trends in veiligheid 2018* (Trends in security 2018) show that 23 percent of the Dutch feel safe and comfortable with the growing number of cameras in public spaces, while 9 percent say they do not.[24] Capgemini also asks people how they feel about the use of sensors to improve safety. Of those surveyed, 78 percent had a positive or very positive opinion of police use of body cams, while 6 percent had a negative or very negative opinion.[25] The survey does not examine the arguments and reasons behind the respondents' views.

24 Hoorweg, E. et al. (2018). Vertrouwen en wantrouwen in de digitale samenleving. Trends in veiligheid 2018. Utrecht: Capgemini, p.4. https://www.capgemini.com/nl-nl/bronnen/visierapport-trends-in-veiligheid-2018/
25 Idem, p.38

There have been few (recent) empirical studies in the Netherlands addressing the public's wishes, concerns and attitudes concerning the use of sensor data to improve safety and quality of life. Research from the 2000s shows that people are more inclined to accept privacy-sensitive interventions when they are used to solve serious crimes, and have a more favourable attitude towards camera surveillance than wiretapping or house searches.[26] They also want to know what happens to their information and for what purpose it is being used, and they see the police as more trustworthy than private security firms.[27]

What research also shows is that people who are more open to sharing information tend to have a more favourable attitude towards using sensors for surveillance purposes than those who are less inclined to share information.[28] One study also shows that gender can influence perceptions: men attach more importance to the party that is using the sensor (such as the police or a private security firm), whereas women consider the purpose of the investigation more important.[29] The sensor application's effectiveness is scarcely relevant:[30] citizens are concerned about the level of personal information being collected and the purpose for which sensor data are used, but they are seemingly less worried about whether the technology actually does what it is supposed to do.

Three personal dimensions

The studies discussed above show that personal traits (such as gender) and general attitudes (such as openness to sharing information) can also play a role in what people think about the use of sensors. Their attitudes can be influenced by three important dimensions of the sensor application, but also by personal dimensions that "colour" their view of an application. Figure 4 illustrates these dimensions as they relate to the subject and the object of perception.

In addition, the societal, cultural and institutional context plays a role in various ways. In a broader sense, this dimension may concern statutory rules for camera surveillance and the general public's trust in or mistrust of the authorities. On a

26 Koops, E.J. & A. Vedder (2001). *Opsporing versus privacy: de beleving van burgers*. The Hague: Sdu Uitgevers; Dinev, T. et al. (2005). 'Internet Users, Privacy Concerns and Attitudes towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States'. *BLED 2005 Proceedings* 30.

27 Schildmeijer, R., C. Samson & H. Koot (2005). *Burgers en hun privacy: opinie onder burgers*. Amsterdam: TNS NIPO Consult.

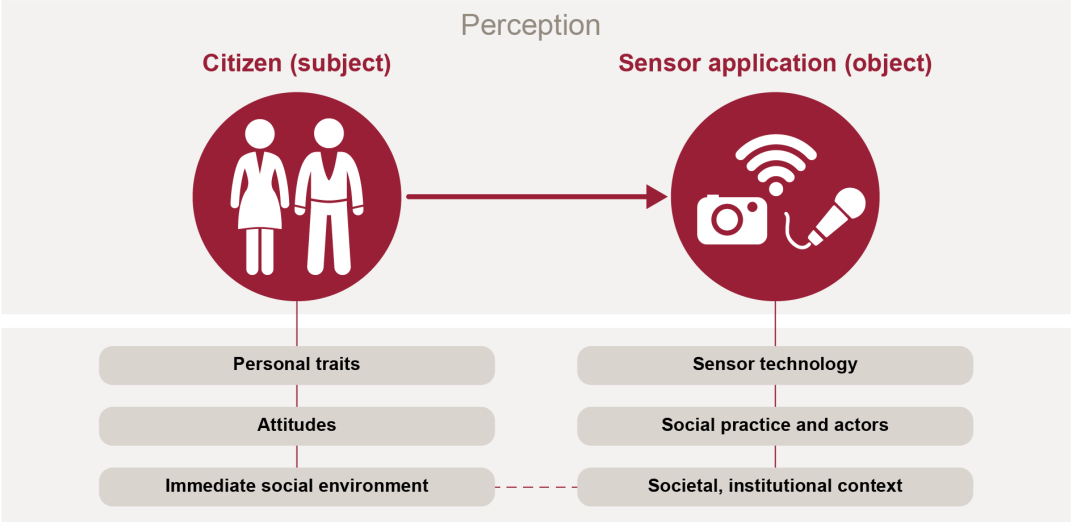
28 Dinev, T. et al. (2005). 'Internet Users, Privacy Concerns and Attitudes towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States'. *BLED 2005 Proceedings* 30.

29 Koops, E.J. & A. Vedder (2001). *Opsporing versus privacy: de beleving van burgers*. The Hague: Sdu Uitgevers.

30 Idem

smaller scale, people's opinions are influenced by their immediate social environment, such as their neighbourhood or their workplace.

Figure 4 Conceptual framework: subject and object dimensions



Source: Rathenau Instituut

Factors identified in European research

Unlike the Netherlands, other countries offer several recent examples of studies examining public attitudes towards sensor applications.[31] Their relevance to our research is limited because of their emphasis on privacy and, in many cases, their American context. However, the European SurPRISE study is of particular interest to the question we are investigating. This study surveys factors that may play a role whether or not the public deems a sensor application acceptable.

SurPRISE in brief

SurPRISE is a recent large-scale research project that examined public acceptance of "Surveillance-Orientated Security Technologies" (SOSTs).[32] Between 2012 and 2015, researchers conducted a quantitative and qualitative study of public acceptance of SOSTs in Austria, Denmark, Germany, Hungary, Italy, Norway,

31 See for example: Potoglou, D. et al. (2017) 'Public preferences for internet surveillance, data retention and privacyenhancing services: Evidence from a pan-European study'. *Computers in Human Behaviour* 75, p.811-825; Rainie, L. M. Duggan. (2016). 'Privacy and information sharing'. Pew Research Center website: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/; Madden, M. L. Rainie. 'Americans' Attitudes About Privacy, Security and Surveillance'. Pew Research Center website: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

32 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*. http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D24-Key-Factors-affecting-public-acceptance-and-acceptability-of-SOSTs-c.pdf

Spain, Switzerland and the United Kingdom. Among other technologies, the study covered (smart) CCTV, biometric identification systems, drones, smartphone location tracking and deep packet inspection (far-reaching analysis of electronic data transmission). Two thousand people (approximately two hundred per country) were interviewed and attended the related participatory events ("Citizen Summits"). Based on an in-depth study of the literature, the SurPRISE researchers identified thirty factors that were thought to affect public acceptance of SOSTs.[33] They then tested these factors empirically.

Factors that influence public acceptance of sensor surveillance

The qualitative SurPRISE study identified seven factors that have a significant impact on people's attitudes towards sensor technologies used for surveillance purposes:

- **General attitude towards SOSTs**: the more that people approve of technology to advance security, the more likely they are to find sensor technologies acceptable. Conversely, the less people approve of technology to advance security, the less likely they are to find sensor technologies acceptable.
- **Institutional trustworthiness**: the higher people perceive the trustworthiness of institutions responsible for sensor technologies, the more likely they are to find the technologies acceptable. Using more acceptable technologies also helps institutions appear more trustworthy.
- **Social proximity**: the more people perceive sensor technologies to be targeted at specific others (such as suspects and criminals), the more acceptable these technologies are compared with blanket surveillance technologies.
- **Perceived intrusiveness**: the more people perceive technologies as intruding into their personal or everyday life, the less likely they are to find them acceptable.
- **Perceived effectiveness**: the more people perceive sensor technologies to be effective, the more likely they are to find them acceptable.
- **Substantial privacy concerns**: the more that people are concerned about their personal data and physical integrity, the less likely they are to find sensor technologies acceptable.
- **Age:** older people are more likely than younger people to accept sensor technologies.

It should be noted that people do not necessarily always realise that these factors influence their opinions, feelings and attitudes.[34] The study further identifies seven factors that have only a minor or indirect influence on public acceptance of sensor

33 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*, p.77

34 Idem, p.80

technologies.[35] The factors "Perceived level of security threat" and "Familiarity with SOSTs" were found to have no significant influence. The same was true of "Income", "Education", "Spatial proximity", "Temporal proximity" and "Risk-benefit balance" (i.e. a trade-off model between privacy and security).

Rules for sensor surveillance

SurPRISE also revealed which conditions or "rules" the public wants to see implemented to make the use of sensors more acceptable.[36] These rules indicate what people consider important in sensor surveillance. During the Citizen Summits organised by the SurPRISE researchers, the participants recommended criteria and put forward arguments underpinning their opinions and feelings about sensor technologies.[37] People find the SOSTs covered by the SurPRISE study more acceptable if:

- they are operated within a European regulatory framework and under the control of a European regulatory body;
- they are operated in a context in which there is transparency about the procedures concerning data protection and accountability;
- they are operated only by public authorities and only for public benefits. Any participation by private actors must be strictly regulated;
- their benefits largely outweigh their costs, especially in comparison to other non-technological, less intrusive, alternatives;
- their operation can be regulated through an opt-in approach;
- they allow monitored individuals to access, modify and delete data about themselves;
- they target less-sensitive data and spaces, whenever possible, according to criteria and purposes which are known to the public;
- they do not operate blanket surveillance but address specific targets, in specific times and spaces and for specific purposes;
- they incorporate privacy-by-design protocols and mechanisms;
- they work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity.

Looking at our conceptual framework, we see that these rules mainly concern the dimension of practices and actors: the way in which sensors are applied in real-life situations, by whom and for what purposes. However, the public also makes demands on the technology itself and the institutional context. People want sensor technology to be designed to exclude privacy issues, for example by minimising data storage, anonymising personal data and encrypting all information. Privacy-by-

35 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: Final publishable summary report,* p.6

36 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*

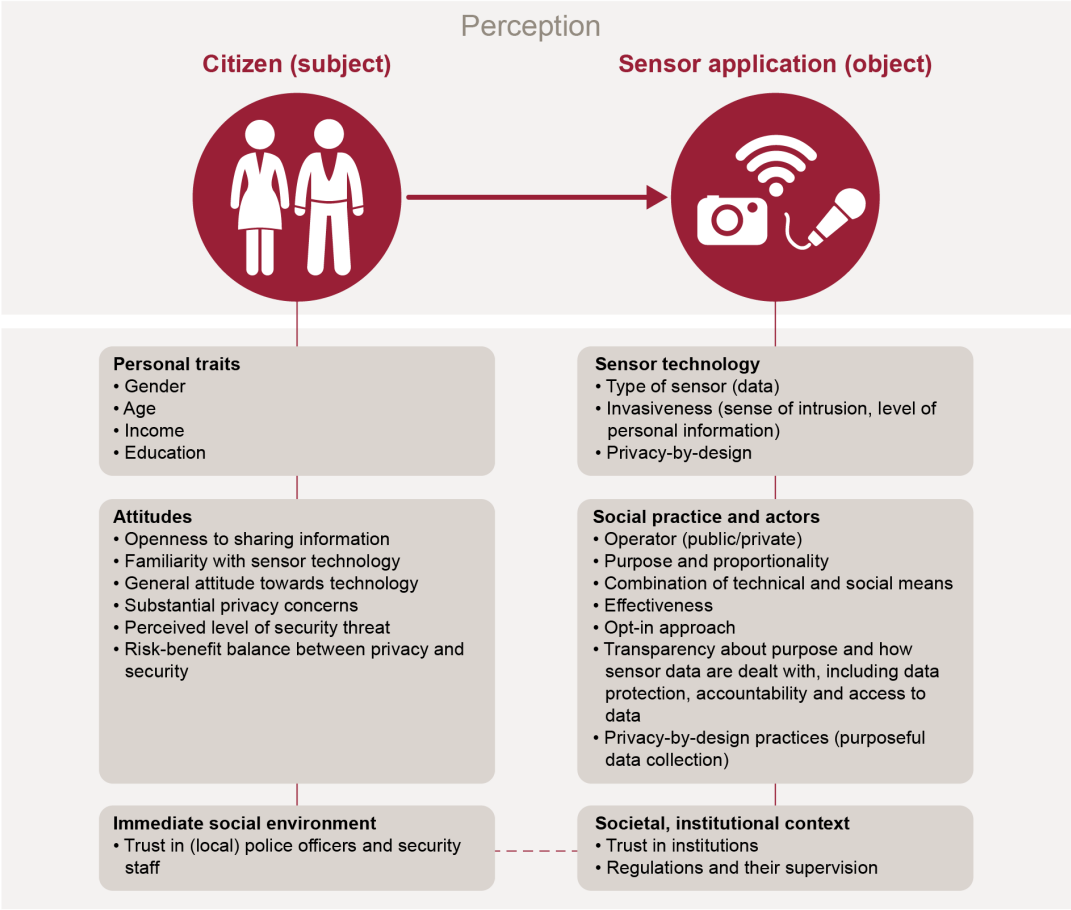
37 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: Final publishable summary report,* p.7

design principles can also be incorporated into the procedures for using sensor technology, for example agreeing to minimise the number of people having access to data. The public also finds the broader institutional context important: the technology must comply with the overarching framework of European rules and supervisory mechanisms. This implies that the public has faith in those rules and trusts that they are monitored properly. These rules are, in turn, transposed into a specific social context.

Survey of factors identified in research

We have sorted the factors from Dutch research and the European SurPRISE study into our conceptual framework. Figure 5 reviews factors taken from research that may affect public perceptions of surveillance using sensors.

Figure 5 Factors identified in research



Source: Rathenau Instituut

Final remarks

In this article, we developed a conceptual framework that helps explain how people form an opinion about the use of sensor technology to improve safety and quality of life. We developed this framework by studying top-down surveillance and differentiate between three personal dimensions and three sensor-related dimensions; all of which can affect people's attitudes. Based on real-life examples and research on public perceptions, we identified factors that may play a role in what people think of sensor surveillance. These factors can be slotted into our conceptual framework; they support that framework and they also help to define it.

What does this mean for our ongoing research? We conclude this article with two thoughts in that regard. First, we show that our framework can be used to examine public perceptions of other types of sensor surveillance. Second, based on our conceptual framework and survey of possible factors, we offer two suggestions that will help us assemble the focus groups.

1. Applying the framework to other types of sensor surveillance

Although we developed our conceptual framework by studying "top-down" surveillance, the framework is also suitable for examining perceptions of other types of sensor surveillance. Below, we show that the three dimensions of sensor applications are also relevant to sousveillance, horizontal surveillance and self-surveillance. This gives us a better understanding of some relevant differences and similarities between the various types of sensor surveillance.

Sensor technology
Different types of sensor surveillance are often based on the same technology. For example, video cameras are used for "top-down" surveillance (CCTV), sousveillance (smartphone cameras) and horizontal surveillance (security cameras at the front door of a private home). There are also differences. The police and the general public may use different sensor technologies, for example.

Social practice and actors
There are key differences between different types of sensor surveillance in the "social practice and actors" dimension. In "top-down" *surveillance*, the government and businesses use cameras and other sensors to keep an eye on the public. Earlier studies have shown that people care about who precisely is collecting and using the sensor data. Is personal information being used by public or private parties, and for public or commercial purposes? Which rules apply to these parties?

Sousveillance is interesting in that the "viewing direction" is reversed: the public operates the camera to keep an eye on the authorities and businesses, for example by videoing police officers or emergency services on the job. The viewing direction changes again in *horizontal surveillance*, with people being videoed by *and* videoing others. In *self-surveillance*, people use sensors to track and monitor themselves (see Figure 2).

These various viewing directions do not only change the operator (the person collecting and using the sensor data) but also the individual about whom sensor data is being collected, as well as the reasons for collecting that information and the purposes that it serves. According to the SurPRISE researchers, these are all factors that may affect whether or not the public finds a sensor application acceptable.

Societal, cultural and institutional context
"Top-down" surveillance relates to trust in the police force or a business, for example. Horizontal surveillance and sousveillance relate to trust in other people, including the question of whether they comply with privacy law, for example. It is also the case that the rules that apply to the police and municipal authorities differ from those that apply to businesses and the general public.

2. Suggestions for the focus groups

We aim to bring together a variety of different opinions and attitudes in the focus groups. We will do this by presenting small groups of ordinary Dutch people with scenarios in which sensors and sensor data are used to improve safety and quality of life. To what extent do ordinary people find these sensor applications acceptable, and why? When do people in fact *expect* sensors to be used to improve safety and quality of life? What reasons, experience and emotions underpin their views? What advantages and disadvantages do they see? We want the focus groups to discuss as many aspects of the perceptions of ordinary Dutch people as they can. Based on our conceptual framework and survey of possible factors, we have developed two suggestions that will help us assemble the focus groups. These suggestions refer to the two basic principles of our conceptual framework: someone (the subject) has an opinion about something (the object). People's perceptions are influenced by their personal traits and by the characteristics of the sensor application:

- **Make sure that the group is diverse and do not lose sight of the individual**
  We are interested in "public perceptions". That sounds abstract, but the point is to examine the opinions and experience of ordinary Dutch people. We have seen that someone's personal traits, general attitudes and immediate social environment may influence their view of sensor applications. Factors such as age, gender, education and the neighbourhood where someone lives may play

a role. These are all aspects that we must bear in mind as we attempt to recruit a diverse group of participants. In addition, it could be useful to examine people's attitudes – for example whether they generally trust the police – before discussing specific sensor applications with them.

- **Ask participants about the key dimensions of sensor applications**
  We can generate diversity in the scenarios by varying the three key dimensions of sensor applications. Public perceptions may concern the sensor technology that is being used, the specific practice and parties that are involved, and the societal, cultural and institutional context. Does it matter to someone what type of sensor data is being collected? Does it matter whether the data are being collected by the police or by a private security firm? How about the person whose data is being collected – is that important? Does the perceived trustworthiness of the local police officer or the police in general play a role? And do "being videoed" and "shooting a video" influence the extent to which people find a sensor application acceptable?

We will use these suggestions to help us develop a method for the focus groups. The police can also use these suggestions when discussing the socially responsible use of sensors and sensor data with persons within and outside their organisation.

The next article will look at the scenarios and questions that we intend to present to the members of the focus groups. One topic that we have not yet addressed in this article is *knowledge*. In everyday life, people are often unfamiliar with all the details of all the dimensions of a sensor application. In our scenarios, we can provide the focus groups with specific information about a situation and see how that influences their expectations regarding the use of sensor data. We will also consider the impact of their expectations on the extent to which they would like to see the applications being used in real-life situations and the extent to which they find an application acceptable or unacceptable. More about that in the next article.

The Rathenau Instituut stimulates public and political opinion forming on social aspects of science and technology. We perform research and organise debate relating to science, innovation and new technologies.

Rathenau Instituut